Amendments to the Claims

Please amend claims 1, 2, 18, 23, 28 and 29. This listing of the claims will replace all prior versions, and listings, of claims in the application.

1. (Currently amended) A system for protecting sensitive information residing in server environments, comprising at least one processing device coupled among at least one network and at least one client computer, wherein the at least one processing device:

receives at least one electronic transaction query from the at least one client computer via at least one secure channel;

~~applies a user-defined pattern matching expression to identify~~ enables a user to specify, via regular expression, a plurality of fields of sensitive data to be encrypted within the at least one electronic transaction query before it reaches components in a server environment;

encrypts the specified sensitive data;

transfers the encrypted sensitive data among components of ~~a~~ the server environment;

receives at least one electronic information query for the encrypted sensitive data from at least one third-party system via the at least one secure channel;

decrypts the encrypted sensitive data in response to the at least one electronic information query; and

provides the decrypted sensitive data to the at least one third-party system via at least one secure coupling.

2. (Currently amended) A method for protecting sensitive information within server environments, comprising:

~~applying a pattern matching expression to identify~~ enabling a user to specify, via regular expression, a plurality of sensitive data elements to be encrypted inside ~~the~~ at least one electronic request before it reaches a server environment;

applying at least one cryptographic operation to the sensitive data specified in response to the at least one electronic request, wherein the sensitive data of the at

least one electronic request is encrypted before transfer among components of the server environment, wherein encrypted sensitive data of the server environment is decrypted before transfer from the server environment.

3. (Original) The method of claim 2, further comprising determining that the at least one electronic request includes sensitive data.

4. (Cancelled)

5. (Original) The method of claim 2, further comprising:

determining that sensitive data in the electronic request includes at least one user password; and

applying at least one hash function to the at least one user password.

6. (Cancelled)

7. (Previously Presented) The method of claim 2, further comprising:

determining the at least one electronic request includes one or more cookies;

identifying at least one cookie of the one or more cookies that includes sensitive data;

applying at least one cryptographic function or checksum to the at least one cookie.

8. (Original) The method of claim 2, wherein the at least one electronic request comprises at least one protocol over Secure Socket Layer.

9. (Original) The method of claim 2, wherein the sensitive data comprises at least one data item selected from a group including credit card numbers, credit card information, account numbers, account information, birth dates, social security numbers, user information, and user passwords.

10. (Original) The method of claim 2, further comprising executing the at least one cryptographic operation using at least one public key.

11. (Original) The method of claim 2, wherein the at least one cryptographic operation includes at least one operation selected from a group including encryption operations, decryption operations, hash operations, keyed hash operations, and keyed hash verification.

12. (Original) The method of claim 2, wherein encrypting includes performing at least one operation on the sensitive data selected from a group including hashing and keyed hashing when the sensitive data is a password.

13. (Original) The method of claim 2, wherein the at least one electronic request comprises at least one encoded key identifier.

14. (Withdrawn) A method for securing sensitive information within server systems, comprising: parsing at least one electronic request received via at least one Internet coupling; dynamically determining that the at least one electronic request includes sensitive data; encrypting the sensitive data; and storing the encrypted sensitive data in at least one component of the server system.

15. (Withdrawn) The method of claim 14, further comprising:

evaluating at least one request for the encrypted sensitive data, wherein the at least one request is received via at least one coupling with at least one third-party system;

decrypting the encrypted sensitive data;

providing the decrypted sensitive data to the at least one coupling with at least one third-party system.

16. (Withdrawn) The method of claim 14, wherein encrypting includes performing at least one operation on the sensitive data selected from a group including hashing and keyed hashing when the sensitive data is a password.

17. (Withdrawn) A method for securing sensitive information within server systems, comprising:

evaluating at least one electronic request received from at least one third-party system via at least one proprietary channel;

dynamically determining the at least one electronic request includes a request for encrypted sensitive data and retrieving the encrypted sensitive data;

decrypting the encrypted sensitive data; and

providing the decrypted sensitive data to the at least one third-party system.

18. (Currently amended) A system for protecting sensitive information within server systems, comprising at least one processing device coupled among at least one server site and at least one client computer and at least one network, wherein the at least one processing device ~~identifies~~ enables a user to specify, using regular expressions, sensitive data to be encrypted inside the electronic request before it reaches components of at least one server system, wherein the at least one processing device applies at least one cryptographic operation to the sensitive data in response to the at least one electronic request, wherein the sensitive data of the at least one electronic request is encrypted prior to transfer among components of the at least one server system, wherein encrypted sensitive data of the at least one server system is decrypted prior to transfer among the at least one network.

19. (Original) The system of claim 18, wherein the at least one processing device determines that the at least one electronic request includes sensitive data by identifying tags indicating that associated data is the sensitive data.

20. (Original) The system of claim 18, wherein the at least one processing device determines that the at least one electronic request includes sensitive data by identifying tags specified by at least one system administrator that associated data is the sensitive data.

21. (Original) The system of claim 18, wherein the sensitive data comprises at least one data item selected from a group including credit card numbers, credit card information, account numbers, account information, birth dates, social security numbers, user information, and user passwords.

22. (Original) The system of claim 18, wherein the at least one cryptographic operation includes at least one operation selected from a group including encryption operations, decryption operations, hash operations, and keyed hash operations.

23. (Currently amended) A cryptographic appliance for securing sensitive information within a server system, comprising: at least one processing device coupled among at least one server system and at least one network coupling to evaluate at least one received electronic request in a first protocol format, wherein the at least one processing device: ~~determines when~~ enables a user to specify, via regular expression, sensitive data to be encrypted in the at least one received electronic request before it reaches components of at least one server system ~~includes sensitive data~~; encrypts the sensitive data; reforms the electronic request, including the encrypted sensitive data, in the first protocol format, and transfers the reformed electronic request among at least one component of the at least one server system.

24. (Original) The cryptographic appliance of claim 23, wherein the at least one processing device: evaluates at least one request for the encrypted sensitive data received via at least one coupling with at least one third-party system; decrypts the encrypted sensitive data; and transfers the decrypted sensitive data to the at least one third-party system.

25. (Cancelled)

26. (Withdrawn) A computer readable medium containing executable instructions which, when executed in a processing system, protects sensitive information within server environments by: evaluating at least one electronic request received over at least one network coupling; dynamically identifying sensitive data inside the electronic request; applying at least one cryptographic operation to the sensitive data in response to the at least one electronic request, wherein sensitive data of the at least one electronic request is encrypted prior to transfer among components of the server environments, wherein encrypted sensitive data of the server environments is decrypted prior to transfer among the at least one network coupling.

27. (Withdrawn) An electromagnetic medium containing executable instructions which, when executed in a processing system, protects sensitive information within server environments by: reading a configuration file to determine how to identify sensitive data within the at least one electronic request received over at least one network coupling; dynamically identifying the sensitive data; and applying at least one cryptographic operation to sensitive data in response to the at least one electronic request, wherein sensitive data of the at least one electronic request is encrypted prior to transfer among components of the server environments, wherein encrypted sensitive data of the server environments is decrypted prior to transfer among the at least one network coupling.

28. (Currently amended) A device for protecting sensitive information within server environments, comprising:

means for receiving at least one electronic transaction query from the at least one client computer via at least one secure coupling;

means for ~~evaluating~~ enabling a user to specify, using a ~~pattern matching~~ regular expression, a plurality of sensitive data to be encrypted in the at least one electronic transaction query before it reaches components of a server environment ~~for sensitive data~~;

means for encrypting ~~detected~~ the specified sensitive data;

means for transferring the encrypted sensitive data among components of the server environment;

means for receiving at least one electronic information query for the encrypted sensitive data from at least one third-party system via the at least one secure coupling;

means for decrypting the encrypted sensitive data in response to the at least one electronic information query; and

means for transferring the decrypted sensitive data to the at least one third-party system via the at least one secure coupling.

29. (Currently amended) A device comprising:

a processor;

a network interface coupled to the processor;

a pattern ~~matching~~ specification engine coupled to the processor,

a cryptographic engine coupled to the processor;

wherein, in operation, first one or more packets including payload formatted in a first protocol are input on the network interface;

the pattern ~~matching~~ specification engine enables a user to apply ~~applies~~ a regular expression ~~pattern~~ to the payload to ~~determine~~ specify which portion of the payload includes sensitive data to be encrypted and which portion of the payload includes non-sensitive data before the payload reaches components of a server environment;

the cryptographic engine applies a cryptographic transformation to the sensitive data;

the processor forms second one or more packets including the cryptographically transformed sensitive data and the non-sensitive data in the first protocol;

the second one or more packets are output on the network interface.

30. (Previously Presented) The device of claim 29, further comprising a database of cryptographic keys, wherein, in operation, the cryptographic engine uses a key from the database of cryptographic keys to cryptographically transform the sensitive data.

31. (Previously Presented) The device of claim 29, wherein the cryptographic transformation includes decryption or encryption.